REMARKS

Claims 1-26 are pending in the current application. In an Office Action dated September 5, 2005 ("Office Action"), the Examiner withdrew the previous office action and reopened prosecution, rejected claims 1-11 and 18-26 under 35 U.S.C. § 102(e) as being anticipated by England et al., U.S. Patent No. 6,938,164 ("England"), and allowed claims 12-17, and allowed claims 12-17. Applicant's representative respectfully traverses the 35 U.S.C. § 102(e) rejections of claims 1-11 and 18-26. Applicant's representative wishes to thank the Examiner for the allowance of claims 12-17, as well as reconsidering the previous office action and searching for the more relevant, currently cited reference.

Claim 1 is provided below, for the Examiner's convenience, as representative of the independent claims of the current application:

> 1. (original) A computer system comprising:
> at least one processor;
> a memory;
> a secure platform stored in the memory for controlling the processor and the memory;
> an operating system image stored in the memory for controlling the processor and the memory and operating on top of the secure platform;
> an end user application stored in the memory for controlling the processor and the memory and operating on top of the operating system image; and
> wherein the secure platform is configured to provide a secure partition within the memory for storing secret data associated with and accessible by the end user application, the secure partition being inaccessible to the operating system and other tasks operating on top of the secure platform.

In the final element of claim 1, a secure memory partition is claimed that is accessible to an end-user application, but not to other tasks executing above the secure platform. Thus, the claimed secure memory partition is accessible only to a single, end-user application. This claimed feature of the disclosed secure-platform-based computer system is important for secure application-program-level computing, and is made possible by the novel, disclosed architecture as well as by architectural features of the Intel Itanium® processor architecture, and by other, similar, modern processor architectures, as described

in the current application, including in the first paragraph of page 35.

England is directed to a rather different system and addresses a different set of problems than those addressed by the secure-platform-based computer system disclosed in the current application. As suggested by the title of England's patent, by England's Abstract, and by England's Summary of the Invention section, England is directed to a code-initialization process. England uses a memory controller to prevent access by CPUs and I/O bus masters to memory during a code initialization process, and once initialization is complete, allows access to memory. As stated by England in the paragraph beginning on line 50 of column 8, England does not specify or care what it is that is initialized. For example, the trusted core that England discusses with regard to one embodiment can be any kind of code. England simply wants to ensure that the code is loaded, and a cryptographic hash generated from the loaded code, before the code can be overwritten or modified by other processes, as discussed in the paragraph beginning on line 6 of column 6 and the paragraph beginning on line 1 of column 9.

In particular, the paragraph of England cited by the Examiner reads as follows:

> In FIG. 3, the trusted core is implemented by establishing two separate "spaces" within computer 100: a trusted space 166 (also referred to as a protected parallel area, or curtained memory) and a normal (untrusted) space 168. These spaces can be, for example, one or more address ranges within computer 100. Both trusted space 166 and normal space 168 include a user space and a kernel space, with the trusted core 170 being implemented in the kernel space of trusted space 166. A variety of trusted applets, applications, and/or agents can execute within the user space of trusted space 166, under control of trusted core 170. However, any application 174, operating system 176, or device driver 178 executing in normal space 168 is prevented, by trusted core 170, from accessing trusted space 166. Thus, no alterations can be made to applications or data in trusted space 166 unless approved by trusted core 170.

This passage does not teach, disclose, or even suggest that England's system provides a protected memory region accessible only to a single end-user application. Instead, England simply discloses a system in which the trusted-core code to be initialized runs from a memory region that is inaccessible, with respect to overwriting or modification, to code running from normal space. There is no teaching or suggestion of secret data

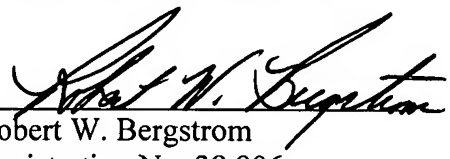
maintained in confidence on behalf of any process in England. In fact, England explicitly states that even:

> the trusted core 146 need not be stored in a secure location and/or loaded into memory 110 in a secure memory. The trusted core 146 may be stored on any publicly-accessible (or semi-publicly accessible) area, such as mass storage device 118, a remote server accessed via network adapter 128, etc. Rather, a cryptographic measure of trusted core 146 can be verified after loading into memory 110 (and after it is protected so that no further modifications by untrusted are possible). (England, column 8, lines 14-22)

Thus, all that the cited passage of England discloses is that the trusted core, and certain other trusted executables, run from a memory region that cannot be altered by executables run from untrusted, normal memory space. There is no mention of secret data, no mention of partitions accessible to only a single end-user process, and no attempt to keep anything, even the trusted core, unreadable by processes or users. Again, England simply wants to ensure that certain code is loaded and a cryptographic hash or digital signature computed for the code, prior to modification or overwriting of the code.

In Applicants' representative's opinion, all of the claims remaining in the application are now clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,
Robert W. Gardner
Olympic Patent Works PLLC



Robert W. Bergstrom
Registration No. 39,906

Enclosures:
Postcard
Transmittal in duplicate

Olympic Patent Works PLLC
P.O. Box 4277
Seattle, WA 98194-0277
206.621.1933 telephone